



COMILLAS
UNIVERSIDAD PONTIFICIA

ICAI

PRÁCTICA 3

Arquitectura de servicios red

Javier Álvarez Martínez
201707599@alu.comillas.edu

1ª SOLUCIÓN

1. Primero permitimos conexiones http a nuestro servicio web en el puerto 80. Conectamos las reglas de firewall a través del network tag, añadiendo el nombre de la regla de firewall.
2. Descargamos nginx(sudo apt install nginx) y llamamos a la IP pública externa de nuestro servidor

34.170.215.16

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

3. Nos conectamos mediante ssh, usando nuestra clave publica a nuestra máquina de salto.

```
C:\Users\javier>ssh 104.154.86.86
The authenticity of host '104.154.86.86 (104.154.86.86)' can't be established.
ECDSA key fingerprint is SHA256:G8EAtt6ra4eRhQ696o4sw0VF93D2owwR1uvkEUBols.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '104.154.86.86' (ECDSA) to the list of known hosts.
Linux maquinasalto 5.10.0-17-cloud-amd64 #1 SMP Debian 5.10.136-1 (2022-08-13) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
javier@maquinasalto:~$
```

4. Nos conectamos a través de la máquina de salto y usando la clave pública de la máquina de salto y mediante ssh a nuestro servicio web.

```
javier@maquinasalto:~$ ssh 10.128.0.5
The authenticity of host '10.128.0.5 (10.128.0.5)' can't be established.
ECDSA key fingerprint is SHA256:mVDmJcJNxVCPo5B3XsyaI7UIqq74TQSiNxU6iMRp/zU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.128.0.5' (ECDSA) to the list of known hosts.
Linux servicioweb 5.10.0-17-cloud-amd64 #1 SMP Debian 5.10.136-1 (2022-08-13) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
javier@servicioweb:~$
```

5. Comprobamos como no nos deja conectarnos a nuestro servicio web a través de un equipo que no sea nuestra máquina de salto

```
C:\Users\javie>ssh 34.170.215.16
ssh: connect to host 34.170.215.16 port 22: Connection timed out
```

6. Mostramos las reglas de firewall creadas.

<input type="checkbox"/>	Nombre	Tipo	Destinos	Filtros	Protocolos/puertos	Acción	Prioridad	Red ↑	Registros	Re
<input type="checkbox"/>	http-servidor	Entrada	http-servicio	Intervalos de	tcp:80	Permitir	1000	default	Desactivado	▼
<input type="checkbox"/>	ssh-salto	Entrada	ssh-salto	Intervalos de	tcp:22	Permitir	1000	default	Desactivado	▼
<input type="checkbox"/>	ssh-servidor	Entrada	ssh-server	Intervalos de	tcp:22	Permitir	1000	default	Desactivado	▼

7. Mostramos las máquinas virtuales

<input type="checkbox"/>	Estado	Nombre ↑	Zona	Recomendaciones	En uso por	IP interna	IP externa	Conectar
<input type="checkbox"/>	✓	maquinasalto	us-central1-a			10.128.0.3 (nic0)	104.154.86.86 (nic0)	SSH ▼
<input type="checkbox"/>	✓	servicioweb	us-central1-a			10.128.0.5 (nic0)	34.170.215.16 (nic0)	SSH ▼

2ª SOLUCIÓN

1. Quitamos la ip pública del servicio web

Editar instancia servicioweb

Edita la interfaz de red

Red *
default

Subred *
default IPv4 (10.128.0.0/20)

La instancia está en ejecución. No se puede cambiar el rango de subred IPv6.

MÁS INFORMACIÓN

Tipo de pila de IP

☒ IPv4 (una sola pila)

☐ IPv4 e IPv6 (pila doble)

Internal IP address
10.128.0.5

IP interna principal
Efímera

Rangos de alias de IP

+ AGREGAR RANGO DE IP

Dirección IPv4 externa
Ninguna

2. Mostramos como no tiene ip externa nuestro servicio web

<input type="checkbox"/>	✓	servicioweb	us-central1-a	10.128.0.5 (nic0)	SSH ▼
--------------------------	---	-----------------------------	---------------	-------------------------------------	-------

3. Demostramos que no podemos conectarnos a internet al quitar la IP pública ya que no podemos descargar nginx.

```
javieservicioweb:~$ sudo apt install nginx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libnginx-mod-http-gzip libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail
  libnginx-mod-stream libnginx-mod-stream-gzip nginx-common nginx-core
Suggested packages:
  nginx-doc ssl-cert
The following NEW packages will be installed:
  libnginx-mod-http-gzip libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail
  libnginx-mod-stream libnginx-mod-stream-gzip nginx-common nginx-core
0 upgraded, 9 newly installed, 0 to remove and 0 not upgraded.
Need to get 1416 kB of archives.
After this operation, 2838 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Err:1 http://deb.debian.org/debian bullseye/main amd64 nginx-common all 1.18.0-6.1+deb11u2
  Could not connect to debian.map.fastlydns.net:80 (199.232.98.132), connection timed out
Err:2 http://deb.debian.org/debian bullseye/main amd64 libnginx-mod-http-gzip amd64 1.18.0-6.1+deb11u2
  Unable to connect to deb.debian.org:http:
Err:3 http://deb.debian.org/debian bullseye/main amd64 libnginx-mod-http-image-filter amd64 1.18.0-6.1+deb11u2
  Unable to connect to deb.debian.org:http:
Err:4 http://deb.debian.org/debian bullseye/main amd64 libnginx-mod-http-xslt-filter amd64 1.18.0-6.1+deb11u2
  Unable to connect to deb.debian.org:http:
Err:5 http://deb.debian.org/debian bullseye/main amd64 libnginx-mod-mail amd64 1.18.0-6.1+deb11u2
  Unable to connect to deb.debian.org:http:
Err:6 http://deb.debian.org/debian bullseye/main amd64 libnginx-mod-stream amd64 1.18.0-6.1+deb11u2
  Unable to connect to deb.debian.org:http:
Err:7 http://deb.debian.org/debian bullseye/main amd64 libnginx-mod-stream-gzip amd64 1.18.0-6.1+deb11u2
  Unable to connect to deb.debian.org:http:
Err:8 http://deb.debian.org/debian bullseye/main amd64 nginx-core amd64 1.18.0-6.1+deb11u2
  Unable to connect to deb.debian.org:http:
Err:9 http://deb.debian.org/debian bullseye/main amd64 nginx all 1.18.0-6.1+deb11u2
  Unable to connect to deb.debian.org:http:
Failed to fetch http://deb.debian.org/debian/pool/main/n/nginx/nginx-common_1.18.0-6.1+deb11u2_all.deb Could not connect to debian.map.fastlydns.net:80 (199.232.98.132), connection timed out
Failed to fetch http://deb.debian.org/debian/pool/main/n/nginx/libnginx-mod-http-gzip_1.18.0-6.1+deb11u2_amd64.deb Unable to connect to deb.debian.org:http:
Failed to fetch http://deb.debian.org/debian/pool/main/n/nginx/libnginx-mod-http-image-filter_1.18.0-6.1+deb11u2_amd64.deb Unable to connect to deb.debian.org:http:
Failed to fetch http://deb.debian.org/debian/pool/main/n/nginx/libnginx-mod-http-xslt-filter_1.18.0-6.1+deb11u2_amd64.deb Unable to connect to deb.debian.org:http:
Failed to fetch http://deb.debian.org/debian/pool/main/n/nginx/libnginx-mod-mail_1.18.0-6.1+deb11u2_amd64.deb Unable to connect to deb.debian.org:http:
Failed to fetch http://deb.debian.org/debian/pool/main/n/nginx/libnginx-mod-stream_1.18.0-6.1+deb11u2_amd64.deb Unable to connect to deb.debian.org:http:
```

```

Failed to fetch http://deb.debian.org/debian/pool/main/n/nginx/nginx-common_1.18.0-6.1%2Bdeb11u2_all.deb Could not connect to debian.map.fastlydns.net:80 (199.232.98.132), connection timed out Could not connect to deb.debian.org:80 (146.75.78.132), connection timed out
Failed to fetch http://deb.debian.org/debian/pool/main/n/nginx/libnginx-mod-http-geoip_1.18.0-6.1%2Bdeb11u2_amd64.deb Unable to connect to deb.debian.org:http:
Failed to fetch http://deb.debian.org/debian/pool/main/n/nginx/libnginx-mod-http-image-filter_1.18.0-6.1%2Bdeb11u2_amd64.deb Unable to connect to deb.debian.org:http:
Failed to fetch http://deb.debian.org/debian/pool/main/n/nginx/libnginx-mod-http-xslt-filter_1.18.0-6.1%2Bdeb11u2_amd64.deb Unable to connect to deb.debian.org:http:
Failed to fetch http://deb.debian.org/debian/pool/main/n/nginx/libnginx-mod-mail_1.18.0-6.1%2Bdeb11u2_amd64.deb Unable to connect to deb.debian.org:http:
Failed to fetch http://deb.debian.org/debian/pool/main/n/nginx/libnginx-mod-stream_1.18.0-6.1%2Bdeb11u2_amd64.deb Unable to connect to deb.debian.org:http:
Failed to fetch http://deb.debian.org/debian/pool/main/n/nginx/libnginx-mod-stream-geoip_1.18.0-6.1%2Bdeb11u2_amd64.deb Unable to connect to deb.debian.org:http:
Failed to fetch http://deb.debian.org/debian/pool/main/n/nginx/nginx-core_1.18.0-6.1%2Bdeb11u2_amd64.deb Unable to connect to deb.debian.org:http:
Failed to fetch http://deb.debian.org/debian/pool/main/n/nginx/nginx_1.18.0-6.1%2Bdeb11u2_all.deb Unable to connect to deb.debian.org:http:
Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
javi@servicioweb:~$

```

4. Utilizamos nat para tener conectividad a internet.

Nombre de la puerta de enlace *

natpuerta ?

Se permiten letras minúsculas, números y guiones

Selecciona Cloud Router ?

Red *

default

Región *

us-central1 (Iowa) ?

Una subred.

Cloud Router *

natrouter ?

5. Vemos como ahora si podemos descargar nginx

```

javi@servicioweb:~$ sudo apt install nginx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libnginx-mod-http-geoip libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip nginx-common
  nginx-core
Suggested packages:
  fcgiwrap nginx-doc ssl-cert
The following NEW packages will be installed:
  libnginx-mod-http-geoip libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip nginx nginx-common
  nginx-core
0 upgraded, 9 newly installed, 0 to remove and 0 not upgraded.
Need to get 1416 kB of archives.
After this operation, 2818 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bullseye/main amd64 nginx-common all 1.18.0-6.1+deb11u2 [126 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 libnginx-mod-http-geoip amd64 1.18.0-6.1+deb11u2 [98.4 kB]
Get:3 http://deb.debian.org/debian bullseye/main amd64 libnginx-mod-http-image-filter amd64 1.18.0-6.1+deb11u2 [102 kB]
Get:4 http://deb.debian.org/debian bullseye/main amd64 libnginx-mod-http-xslt-filter amd64 1.18.0-6.1+deb11u2 [100 kB]
Get:5 http://deb.debian.org/debian bullseye/main amd64 libnginx-mod-mail amd64 1.18.0-6.1+deb11u2 [129 kB]
Get:6 http://deb.debian.org/debian bullseye/main amd64 libnginx-mod-stream amd64 1.18.0-6.1+deb11u2 [155 kB]
Get:7 http://deb.debian.org/debian bullseye/main amd64 libnginx-mod-stream-geoip amd64 1.18.0-6.1+deb11u2 [97.6 kB]
Get:8 http://deb.debian.org/debian bullseye/main amd64 nginx-core amd64 1.18.0-6.1+deb11u2 [515 kB]
Get:9 http://deb.debian.org/debian bullseye/main amd64 nginx all 1.18.0-6.1+deb11u2 [92.9 kB]
Fetched 1416 kB in 15s (91.6 kB/s)
Preconfiguring packages ...
Selecting previously unselected package nginx-common.
(Reading database ... 53996 files and directories currently installed.)
Preparing to unpack .../0/nginx-common_1.18.0-6.1+deb11u2_all.deb ...
Unpacking nginx-common (1.18.0-6.1+deb11u2) ...
Selecting previously unselected package libnginx-mod-http-geoip.
Preparing to unpack .../1/libnginx-mod-http-geoip_1.18.0-6.1+deb11u2_amd64.deb ...
Unpacking libnginx-mod-http-geoip (1.18.0-6.1+deb11u2) ...
Selecting previously unselected package libnginx-mod-http-image-filter.
Preparing to unpack .../2/libnginx-mod-http-image-filter_1.18.0-6.1+deb11u2_amd64.deb ...
Unpacking libnginx-mod-http-image-filter (1.18.0-6.1+deb11u2) ...
Selecting previously unselected package libnginx-mod-http-xslt-filter.
Preparing to unpack .../3/libnginx-mod-http-xslt-filter_1.18.0-6.1+deb11u2_amd64.deb ...
Unpacking libnginx-mod-http-xslt-filter (1.18.0-6.1+deb11u2) ...
Selecting previously unselected package libnginx-mod-mail.
Preparing to unpack .../4/libnginx-mod-mail_1.18.0-6.1+deb11u2_amd64.deb ...
Unpacking libnginx-mod-mail (1.18.0-6.1+deb11u2) ...
Selecting previously unselected package libnginx-mod-stream.
Preparing to unpack .../5/libnginx-mod-stream_1.18.0-6.1+deb11u2_amd64.deb ...
Unpacking libnginx-mod-stream (1.18.0-6.1+deb11u2) ...
Selecting previously unselected package libnginx-mod-stream-geoip.
Preparing to unpack .../6/libnginx-mod-stream-geoip_1.18.0-6.1+deb11u2_amd64.deb ...
Unpacking libnginx-mod-stream-geoip (1.18.0-6.1+deb11u2) ...
Selecting previously unselected package nginx-core.
Preparing to unpack .../7/nginx-core_1.18.0-6.1+deb11u2_amd64.deb ...
Unpacking nginx-core (1.18.0-6.1+deb11u2) ...
Selecting previously unselected package nginx.
Preparing to unpack .../8/nginx_1.18.0-6.1+deb11u2_all.deb ...
Unpacking nginx (1.18.0-6.1+deb11u2) ...
Setting up nginx-common (1.18.0-6.1+deb11u2) ...
Setting up libnginx-mod-http-xslt-filter (1.18.0-6.1+deb11u2) ...
Setting up libnginx-mod-http-geoip (1.18.0-6.1+deb11u2) ...
Setting up libnginx-mod-mail (1.18.0-6.1+deb11u2) ...
Setting up libnginx-mod-http-image-filter (1.18.0-6.1+deb11u2) ...
Setting up libnginx-mod-stream (1.18.0-6.1+deb11u2) ...
Setting up libnginx-mod-stream-geoip (1.18.0-6.1+deb11u2) ...
Setting up nginx-core (1.18.0-6.1+deb11u2) ...
Upgrading binary: nginx.
Setting up nginx (1.18.0-6.1+deb11u2) ...
Processing triggers for man-db (2.9.4-2) ...

```


6. Creamos balanceador de cargas. Primeramente, debemos configurar el frontend de nuestro balanceador, queremos utilizar un protocolo HTTPS y con una ip estática.

Configuración de frontend

Configura la dirección IP, el puerto y el protocolo del frontend del balanceador de cargas.

IP y puerto de frontend nuevos

Nombre

frontend

Minúsculas, sin espacios.

Protocolo

HTTPS (incluye HTTP/2)

Selecciona HTTPS para admitir clientes que admitan HTTP/2. El balanceador de cargas ofrece automáticamente HTTP/2 como parte del protocolo de enlace TLS.

Versión de IP

IPv4

IP address

ipestatica

Puerto

443

El balanceo de cargas HTTPS global solo admite el puerto TCP 443.

A continuación, debemos crearnos un certificado con el objetivo de que sea lo más fiable posible permitiendo https.

[illegible]

Crear un certificado

Nombres de host de DNS	Javi
Vencimiento	✓ 19 sept 2023 11:01:52
Número de serie	5BDD3A5E028F466A7F901 9250B30F39E21DE7ABF
Emitor de certificados	Javi

Crear modo

- ☒ Subir certificado

Usa tus propios certificados de clave pública, cadenas de certificados y claves privadas
- ☐ Crear certificado administrado por Google

Google aprovisionará automáticamente un certificado SSL una vez que finalices la configuración de LB y dirijas el DNS de todos los dominios especificados a la IP asociada con el balanceador de cargas

Certificado *

```
N/1EJl5x9zo9TRPFzKC
x3ElurY0tuFOfojHzXNzkSxBIQ==
-----END CERTIFICATE-----
```

[SUBIR](#)

Clave privada *

```
4urWJdZMYid
VlhdmYUdyjySAIcKOZiveT4
-----END PRIVATE KEY-----
```

[SUBIR](#)

A continuación, configuramos el backend de nuestro loadbalancer.

Nombre *

backend

Minúsculas, sin espacios.

Descripción

Tipo de backend

Grupo de extremos de red zonal

Protocolo

HTTP

Puerto con nombre

http

Tiempo de espera *

30

segundos

Backends

Regiones

us-central1

Nuevo backend

Grupo de extremos de red *

networkgroup

Modo de balanceo

Tasa

Máximo de RPS *

10

RPS

Alcance

por extremo

Capacidad *

100

%

CANCELAR

LISTO

Creamos el health checker:

Verificación de estado

Nombre *

healthcheck

Minúsculas, sin espacios.

Descripción

Protocolo

TCP

Especificación de puerto

Puerto de servicio

Protocolo de proxy

PROXY_V1

Solicitar

Respuesta

Registros

- ☐ Activado
- Activar los registros de verificación de estado puede aumentar los costos en Cloud Logging.
- ☒ Desactivado

Criterios de buen estado

Define cómo se determina el estado: con cuánta frecuencia se verifica, cuánto tiempo se debe esperar una respuesta y cuántos intentos exitosos o con errores son decisivos.

Intervalo de verificación *

5

segundos

Tiempo de espera *

5

segundos

Umbral de buen estado *

2

resultados correctos consecutivos

Umbral de mal estado *

2

errores consecutivos

Verificamos que esta creado correctamente

<input type="checkbox"/>	Nombre	Tipo de balanceador de cargas	↑	Protocolos	Región	Backends	
<input type="checkbox"/>	frontend-redirect	HTTP(S)		HTTP			
<input type="checkbox"/>	loadbalancer	HTTP(S)		HTTPS		1 servicio de backend (0 grupos de instancias, 1 grupo de extremos de red)	

loadbalancer

Rendimiento web más rápido y mayor protección web con Cloud CDN y Cloud Armor. [Más información](#)

DETALLES

MONITORING

ALMACENAMIENTO EN CACHE

Frontend

Protocolo	↑	IP/Puerto	Certificado	Política de SSL	Nivel de red
HTTPS		34.160.158.197:443	certificado	Predeterminada de GCP	Premium

Normas de enrutamiento

Hosts	↑	Rutas	Backend
Todos los que no coincidan (predeterminado)		Todos los que no coincidan (predeterminado)	backend

Backend

Servicios de backend

1. backend

Protocolo de extremo	Tiempo de espera	Verificación de estado	Cloud CDN	Registros
HTTP	30 segundos segundos	healthcheck	Inhabilitada	Inhabilitada

CONFIGURACIÓN AVANZADA

Nombre	↑	Tipo	Alcance	En buen estado	Ajuste de escala automático	Modo de balanceo	Capacidad
networkgroup		Grupo de extremos de red zonal	us-central1-a	1 de 1	Sin configuración	RPS máximas: 10 (por extremo)	100%

A continuación, queremos establecer unas normas de seguridad para nuestro servidor web, tanto de SQL Injection, Cross Syte Scripting y restricción de tráfico a países de confinaza de la Unión europea. Para ello accedemos a Cloud Armor de Google.

En primer lugar, configuramos las reglas para evitar SQL Injection.

Nueva norma ^

Descripción
SQL Injection 13 / 64

Condición ?

Modo

☐ Modo básico (solo direcciones o rangos de IP) ?

☒ Modo avanzado ?

Coincidencia ?

Presiona Ctrl + Espacio para obtener sugerencias en el editor

```
1 evaluatePreconfiguredExpr('sqli-v33-stable')
```

AYUDA DE LA SINTAXIS DE REGLAS

Acción *

Denegar

Código de respuesta *

403 (Prohibido)

☐ Habilitar solo vista previa

Prioridad *

1

A continuación, configuramos la regla para evitar Cross Syte Scripting.

Descripción
XSS 3 / 64

Condición ?

Modo

☐ Modo básico (solo direcciones o rangos de IP) ?

☒ Modo avanzado ?

Coincidencia ?

Presiona Ctrl + Espacio para obtener sugerencias en el editor

```
1 evaluatePreconfiguredExpr('xss-v33-stable')
```

AYUDA DE LA SINTAXIS DE REGLAS

Acción *

Denegar

Código de respuesta *

403 (Prohibido)

☐ Habilitar solo vista previa

Prioridad *

2

Por último, restringimos el tráfico a los países amigos de la Unión Europea.

Descripción

countries restriction

21 / 64

Condición

Modo

Modo básico (solo direcciones o rangos de IP)

Modo avanzado

Coincidencia

Presiona Ctrl + Espacio para obtener sugerencias en el editor

Presiona Alt + F1 para ver las opciones de accesibilidad.

1

'[AD,AT,BE,CH,DE,DK,EE,ES,FI,FR,GR,IT,HR,IR,GB,NL,PT]'...

contains(origin.region_code)

AYUDA DE LA SINTAXIS DE REGLAS

Acción *

Permitir

Inserta un encabezado

+ AGREGAR ENCABEZADO

☐ Habilitar solo vista previa

Prioridad *

0

☐ securepolicy

Política de seguridad del backend

4

0

Una vez tenemos la política de seguridad creada, lo añadimos a nuestro backend del load balancer.

Editar servicio de backend

☐ Habilitar Cloud CDN

Modo de almacenamiento en caché

De forma predeterminada, Cloud CDN almacenará en caché el contenido estático, incluidos los elementos web y los archivos de video, que no se marque de forma explícita como privado para el tiempo de actividad (TTL) predeterminado que se estableció, sin requerir ningún cambio en tu origen.

Contenido estático en caché (opción recomendada)

Usar configuración de origen en función de los encabezados de control de caché

Forzar el almacenamiento en caché de todo el contenido

El origen debe establecer encabezados

Almacena en caché todo el contenido que entrega el origen, sin importar las directivas "private", "no-store" o "no-cache".

Tiempo de actividad del cliente

1 hora

Tiempo de actividad predeterminado

1 hora

Tiempo de actividad máximo

1 día

Clave de caché

Predeterminada (incluye todos los componentes de una URL de solicitud)

Verificación de estado *

healthcheck

especificación de puerto: puerto de servicio, tiempo de espera: 5 s, intervalo de verificación: 5 s, umbral de mal estado: 2 intentos

Registro

☐ Habilitar registro

Seguridad

Política de seguridad de backend de Cloud Armor

securepolicy

Política de seguridad perimetral de Cloud Armor

CONFIGURACIÓN AVANZADA

Para demostrar que funciona correctamente, nos conectamos a través de nuestro navegador a la dirección pública de nuestro load balancer redirect. De esta forma se puede ver lo siguiente:

⚠ No es seguro | <https://34.160.158.197>

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

Pone que no es seguro porque la certificación está hecha por nosotros mismos, es decir, lo hemos auto firmado y no es una autoridad reconocida por nuestro navegador.

Para comprobar que las reglas funcionan correctamente vamos a eliminar de la lista de países permitidos a España, de esta manera no podremos conectarnos a nuestro servicio web.



⚠ No es seguro | <https://34.160.158.197>

403 Forbidden

¿Qué ventajas e inconvenientes tiene hacer http offloading en el balanceador?

La principal ventaja que tiene utilizar SSL offloading es que el servidor no necesita descifrar y cifrar todos los datos entrantes y salientes, esto permite reducir la carga de trabajo, es decir, nos permite mejorar la velocidad de nuestros servidores.

La desventaja principal es que el tráfico entre el load balancer y el servidor no está cifrado y por lo tanto es vulnerable al robo de datos, al secuestro de sesiones e incluso ataques Man in the middle y además compartir la clave privada del servidor con el load balancer puede ser arriesgado.

¿Qué pasos adicionales has tenido que hacer para que la máquina pueda salir a internet para poder instalar el servidor nginx?

Al eliminar la ip pública de nuestro servidor web no tenemos acceso a Internet y por tanto no podemos instalar nginx. Para solucionar este problema y como queremos evitar otorgar una ip pública a dicho servidor, implementamos un mecanismo de NAT, un mecanismo utilizado por routers IP para cambiar paquetes entre dos redes que asignan redes incompatibles.

Una vez implementado el mecanismo ya tenemos la posibilidad de conectarnos a la red, sin haber otorgado una dirección ip pública, y de este modo poder descargar nginx.

4ª SOLUCIÓN

¿Qué otras mejoras se te ocurrirían para mejorar la seguridad o disponibilidad del servidor web?

Para mejorar la seguridad podríamos mejorar la funcionalidad de nuestro servicio de seguridad, por ejemplo, implementando nuevas reglas WAF a nuestro cloud armour. En este caso se sugiere la implementación de una regla que evite la detección de escáner. Este ataque, también conocido como port scan consiste en analizar de forma automática todos los puertos de un equipo que esté conectado a la red buscando posibles puertos que estén abiertos o con protocolos de seguridad deficientes para llevar a cabo sus ataques.

Otra posibilidad sería la de implementar protección frente a la inclusión de archivos remotos. Este ataque consiste en incluir archivos maliciosos externos que posteriormente son ejecutados por la web o por una aplicación.

Para mejorar la disponibilidad de nuestro servidor web sería una buena idea levantar el servidor en una zona y los back-up de nuestro servidor en zonas distintas, de este modo si ocurre un problema en una zona determinada podríamos levantar el servidor preparado como back-up y continuar con el servicio.